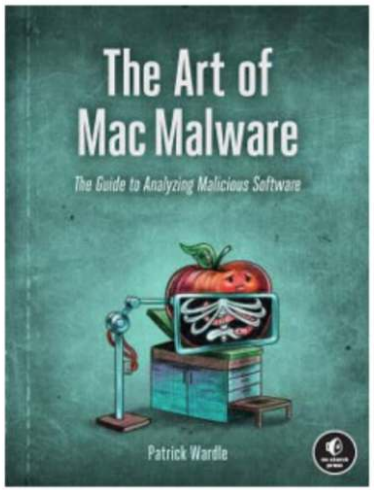

Patrick Wardle

The Art of Mac Malware

The Guide to Analyzing Malicious Software

No Starch Press 2022
328 Seiten
Taschenbuch 37,99 €
E-Book 28,49 €

Patrick Wardle, ehemaliger NSA-Hacker und Gründer von Objective-See, einer Non-Profit-Organisation für Open-Source-Sicherheitssoftware, hat „The Art of Mac Malware" dreigeteilt angelegt. Im ersten Teil stellt er Basiswissen zum Thema vor – Infektionsvektoren, Persistierungsmethoden, Leistungsfähigkeit der Schädlinge. Im zweiten Teil geht es um die Analyse der Schadsoftware sowie statische und dynamische Analysetools. Konkret wird es im dritten Teil. Hier wird die bekannte Malware EvilQuest analysiert und das theoretisch Gelernte praktisch erprobt. Da es sich um echte Schadsoftware handelt, ist äußerste Vorsicht geboten: separater Rechner, kein Filesharing sowie Internetverbindung nur per VPN, um das Nachladen einer Payload oder die Übermittlung von Daten zu verhindern. Eine VM komme nicht infrage, da schon Malware aus einem VM-Container ausgebrochen sei, etwa aus der JavaScript-Sandbox vm2.

Den breitesten Raum im Buch nimmt die Untersuchung von Schadcode ein. Hierzu erklärt Wardle zunächst einfache Bordmittel wie `Hexdump` oder das `File`-Kommando sowie das Objective-See-Tool `WhatsYourSign`. Selbstredend, dass auch DMGs, PKGs, Skripte und Microsoft-Office-Dokumente behandelt werden. Viele Mac-Schädlinge sind laut Wardle in Mach-O-Binaries hineinkompiliert, deren Analyse spezielle Tools benötigt. So lässt sich mittels `MachOView` ein Einblick in solche Binaries gewinnen. Zudem sei Mach-O-Malware oft in Objective-C geschrieben, sodass Klasseninformationen mittels `class-dump` ans Tageslicht kommen, sofern der Code nicht obfuskiert ist.

Wenn feststehen sollte, dass eine Binärdatei bösartig ist, aber keinem bekannten Schädling ähnelt, bleibt Reverse Engineering mittels eines Disassemblers. Dafür stellt Wardle die Assembler-Basics der x86-Architektur vor und verweist auf Literatur dazu. Die ARM-basierte Prozessorarchitektur Apple Silicon spart er aus, da die allermeiste Schädlingssoftware für Intel geschrieben ist und zudem derzeit Programme als Universal Binary ausgeliefert werden, sodass Intel- und ARM-Zweig identisch sind. Es schließt sich eine praktische Unterweisung in `LLDB` als Debugger an. Alle Kapitel enden mit einer kurzen Zusammenfassung des Inhalts und einer Kurzvorstellung des nächsten Kapitels. Zahlreiche Screenshots und Listings erleichtern das Erarbeiten des Stoffes. Patrick Wardle erteilt der Vorstellung, Macs seien sicherer als Windows-Systeme, schon im Vorwort eine klare Absage. Ob man jetzt anhand seines Buchs sicher Bedrohungsvektoren erkennen, analysieren und bannen kann, sei dahingestellt. Das hängt vom Vorwissen ab und der Fähigkeit, das Dargebotene für sich selbst praktisch umzusetzen. Auf alle Fälle schärft Wardle aber das Verständnis für das Thema Mac-Schädlinge und erhöht die nötige Wachsamkeit.

Karsten Kisser (js@ix.de)